ID - 201901100

Page No.:

Date:

SC-402 Assignment 1

[1] We got 26 solutions for keys x=0 to x=26.
Among them,
The answer is found for key x=16 and which is LOOK UP IN THE AIR ITS A BIRD ITS A PLANE ITS SUPERMAN.

[2] $\mathbb{Z}_m$ for $m = 30; 100; 1225$

- for $m = 30$
$30 = 2 \times 3 \times 5$
$\phi(30) = 1 \times 2 \times 4 = 8$
number of keys in affine cipher=
$30 \times 8 = 240$
- for $m = 150$
$100 = 2 \times 2 \times 5 \times 5$
$\phi(100) = (4-2) \times (25-5) = 40$
number of keys in affine cipher $= 4000$
- for $m = 1225$
$1225 = 5 \times 5 \times 7 \times 7$
$\phi(1225) = (25-5) \times (49-7) = 840$
number of keys in affine cipher =
$1225 \times 840 = 1029000$

[3] Z_m for m = 28, 33, 35

- for Z_{28},
  invertible elements = 1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27
- for Z_{33},
  invertible elements = 1, 2, 4, 5, 7, 8, 10, 13, 14, 16, 17, 19, 20, 23, 25, 26, 28, 29, 31, 32
- for Z_{35},
  invertible elements = 1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34

[4] (a)

π^{-1} will be

1	2	3	4	5	6	7	8
2	4	6	1	8	3	5	7

(b)

T G E E M N F L	G E N T E E M L
1 2 3 4 5 6 7 8	2 4 6 1 8 3 5 7
N N T D R O E O	N D O N O T R E
1 2 3 4 5 6 7 8	2 4 6 1 8 3 5 7

AAHDOETC ADEACHOT
1 2 3 4 5 6 7 8 2 4 6 1 8 3 5 7

SHAEIRLM HETSMAIL
1 2 3 4 5 6 7 8 2 4 6 1 8 3 5 7

final encoded form will be
GENTEEML NDONOTRE ADEACHOT
HETSMAIL

[5] our decipher requires $12/m \geq m$,
so m can only be 1, 2 or 3.

- for m=2, the key is not constant
so we will check for m=3.
Here, we will check for 9 characters
to construct matrix and last 3
characters, ~~will be~~
We will check the constructed matrix
is correct or not.
- Construct the matrix,
$K=(1\ 17\ 4 : 0\ 19\ 7 : 19\ 0\ 10)^{-1} \times (17\ 20\ 15 : 14\ 19\ 4 : 13\ 19\ 14)$
So, matrix $K=(3\ 21\ 20 : 4\ 15\ 23 : 6\ 14\ 5)$

[6] From the question,

- $X_1 = (0, 3, 8)$, $X_2 = (18, 15, 11)$, $X_3 = (0, 24, 4)$
  $X_4 = (3, 4, 16)$, $X_5 = (20, 0, 9)$, $X_6 = (8, 14, 13)$
- $Y_1 = (3, 18, 17)$, $Y_2 = (12, 18, 8)$, $Y_3 = (14, 15, 11)$
  $Y_4 = (23, 11, 9)$, $Y_5 = (1, 25, 20)$, $Y_6 = (11, 11, 12)$
- for $1 \leq l \leq 16$, it holds $Y_i = X_i \times l + b$.
  therefore $1 \leq l \leq 3$, we have
  $Y_i - Y_4 = (X_i - X_4) \times L$
- we form the matrix of 3×3, y' having rows $Y_i - Y_4$ $(1 \leq l \leq 3)$
  and then $L = (x')\,l\,y'$.
- once we ~~find~~ found L, we can determine b.
- $b = Y_i - X_i L$
- we have, $x' = (23, 15, 18 ; 15, 11, 21 ; 23, 20, 14)$
  $y' = (6, 7, 8 ; 15, 7, 25 ; 17, 4, 2)$
- So L will be $(3 \; 6 \; 4 ; 5 \; 15 \; 18 ; 17 \; 8 \; 5)$
  then $b = (8 \; 31 \; 1)$

[7] we get plain text for all keys from 'a' to 'z'.
Among them, 't' gives meaningful plaintext which is 'there is no time like the present.'